# Bounded Satisfiablity for PCTL

Nathalie Bertrand, John Fearnley and Sven Schewe

Inria Rennes - University of Liverpool

CSL 2012

# Probabilistic Computation Tree Logic

Variant of CTL with probabilistic path quantifiers.

- A deadlock is reached with probability no more than 0.6: $\mathbb{P}_{\leq 0.6}(\Diamond \text{deadlock})$
- Almost surely whenever a message is sent, with probability more than 0.9 it will be delivered within the next 3 discrete steps: $\mathbb{P}_{=1}(\Box \text{sent} \rightarrow \mathbb{P}_{>0.9}(\Diamond^{\leq 3} \text{received}))$

# Probabilistic Computation Tree Logic

Variant of CTL with probabilistic path quantifiers.

- A deadlock is reached with probability no more than 0.6: $\mathbb{P}_{\leq 0.6}(\Diamond \text{deadlock})$
- Almost surely whenever a message is sent, with probability more than 0.9 it will be delivered within the next 3 discrete steps: $\mathbb{P}_{=1}(\Box \text{sent} \rightarrow \mathbb{P}_{>0.9}(\Diamond^{\leq 3} \text{received}))$

## Syntax of PCTL

- state formulae: $\psi ::= \texttt{tt} \,|\, a \,|\, \psi_1 \wedge \psi_2 \,|\, \neg \psi \,|\, \mathbb{P}_{\bowtie \lambda}(\varphi)$
- path formulae: $\varphi ::= \bigcirc \psi \,|\, \psi_1 \mathsf{U} \psi_2 \,|\, \psi_1 \mathsf{U}_{\leq n} \psi_2 \,|\, \Box \psi \,|\, \Diamond \psi \cdots$

$$s \models \mathbb{P}_{\bowtie \lambda}(\varphi) \quad \text{iff} \quad Pr(s \models \varphi) \bowtie \lambda$$

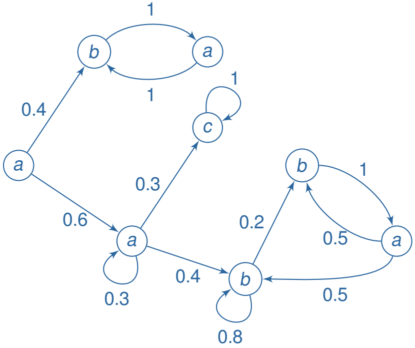
# Markov chains

PCTL models: Markov chains

**Discrete time Markov chain**

$\mathcal{M} = (S, \mathbf{P}, L)$

- $S$ set of states
- $\mathbf{P}$ probability matrix
- $L : S \to 2^{AP}$ labelling function



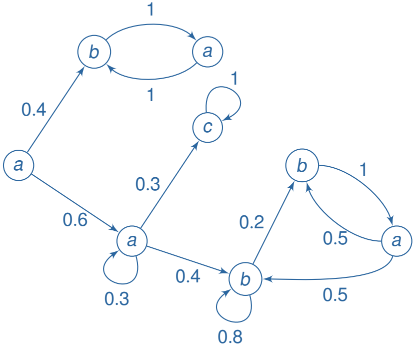
# Markov chains

PCTL models: Markov chains

**Discrete time Markov chain**

$\mathcal{M} = (S, \mathbf{P}, L)$

- $S$ set of states
- $\mathbf{P}$ probability matrix
- $L : S \to 2^{AP}$ labelling function




**PCTL model checking for Markov chains**

Linear in $|\varphi|$ and polynomial in $|\mathcal{M}|$.

Mature tools: *e.g.* PRISM, MRMC.

# PCTL satisfiability

Longstanding open problem!

# PCTL satisfiability

Longstanding open problem!

Qualitative PCTL: thresholds 0 and 1 only.

**Decidability for qualitative fragment** [BFKK08]

Satisfiability for qualitative PCTL is EXPTIME-complete.

# PCTL satisfiability

Longstanding open problem!

Qualitative PCTL: thresholds 0 and 1 only.

**Decidability for qualitative fragment** [BFKK08]

Satisfiability for qualitative PCTL is EXPTIME-complete.

$\mathbb{P}_{=1}(\Box \mathbb{P}_{>0}(\bigcirc a)) \wedge \mathbb{P}_{>0}(\Box \neg a)$ is satisfiable but has no finite model.

# Simple models

## Simple Markov chains

$\mathcal{M} = (S, \mathbf{P}, L)$ is *simple* if

- $L$ has a special atomic proposition $a_{\text{real}}$,
- coefficients in $\mathbf{P}$ belong to $\{0, \frac{1}{2}, 1\}$.

Representation: graph where each vertex has 2 successors.

# Simple models

## Simple Markov chains

$\mathcal{M} = (S, \mathbf{P}, L)$ is *simple* if

- $L$ has a special atomic proposition $a_{\text{real}}$,
- coefficients in $\mathbf{P}$ belong to $\{0, \frac{1}{2}, 1\}$.

Representation: graph where each vertex has 2 successors.

Simple Markov chains can simulate rational probabilities.

PCTL semantics: only real states matter.

# Problem statement

Only implementable and small models are interesting to practitioners!

## Bounded satisfiability problem

Given $\psi$ a PCTL formula and $b \in \mathbb{N}$ a size bound, does $\psi$ have a **simple** model with **at most** $b$ **states**?

# Problem statement

Only implementable and small models are interesting to practitioners!

## Bounded satisfiability problem

Given $\psi$ a PCTL formula and $b \in \mathbb{N}$ a size bound, does $\psi$ have a **simple** model with **at most** $b$ **states**?

## Complexity

Bounded satisfiability is an NP-complete problem in the joint size of $\psi$ and $b$.
Approximating the size of the smallest simple model of $\psi$ within a factor polynomial in $|\psi|$ is NP-hard.

# Reduction to SMT

SMT: Is a logical formula in boolean logic with additional theories satisfiable?

Theories: linear real arithmetic and uninterpreted function symbols

# Reduction to SMT

SMT: Is a logical formula in boolean logic with additional theories satisfiable?

Theories: linear real arithmetic and uninterpreted function symbols

From $\psi$ and *b*, build $C$ set of SMT constraints s.t.
$\psi$ has a simple model with *b* states $\iff C$ is satisfiable

$\rightarrow$ Linear time transformation

Run `Yices` SMT solver on $C$: unsat or sat + model description

# Encoding a simple Markov chain

- $\texttt{States} = \{1, \cdots, b\}$
- $\texttt{left} : \texttt{States} \rightarrow \texttt{States}$, $\texttt{right} : \texttt{States} \rightarrow \texttt{States}$
- $\texttt{real} : \texttt{States} \rightarrow \mathbb{B}$
- $\texttt{truth}_a : \texttt{States} \rightarrow \mathbb{B}$, for each atomic proposition $a$

# Encoding a simple Markov chain

- $\texttt{States} = \{1, \cdots, b\}$
- $\texttt{left} : \texttt{States} \to \texttt{States}$, $\texttt{right} : \texttt{States} \to \texttt{States}$
- $\texttt{real} : \texttt{States} \to \mathbb{B}$
- $\texttt{truth}_a : \texttt{States} \to \mathbb{B}$, for each atomic proposition $a$
- Finitely many hidden states between two real states.
  $\texttt{dist} : \texttt{States} \to [0, 1]$
  - $\forall s\ \texttt{real}(s) \leftrightarrow \texttt{dist}(s) = 0$
  - $\forall s\ \neg\texttt{real}(s) \to$
    $\big(\texttt{dist}(s) > \texttt{dist}(\texttt{left}(s))\big) \vee \big(\texttt{dist}(s) > \texttt{dist}(\texttt{right}(s))\big)$

# Encoding a PCTL formula

$\mathtt{sat}_\phi : \mathtt{States} \rightarrow \mathbb{B}$, $\forall \phi$ subformula of $\psi$

- constraints on $\mathtt{sat}_\phi$ depend on the type of $\phi$

# Encoding a PCTL formula

$\mathtt{sat}_\phi : \mathtt{States} \rightarrow \mathbb{B}$, $\forall\phi$ subformula of $\psi$

- constraints on $\mathtt{sat}_\phi$ depend on the type of $\phi$

- Next operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\bigcirc\phi')$
  - $\forall s\ \mathtt{sat}_\phi(s) \leftrightarrow \frac{1}{2} \cdot \Big(\mathtt{sat}_{\phi'}(\mathtt{left}(s)) + \mathtt{sat}_{\phi'}(\mathtt{right}(s))\Big) \bowtie \lambda$

# Encoding a PCTL formula

$\mathtt{sat}_\phi : \mathtt{States} \rightarrow \mathbb{B}$, $\forall \phi$ subformula of $\psi$

- constraints on $\mathtt{sat}_\phi$ depend on the type of $\phi$

- Next operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\bigcirc\phi')$
  - ~~$\forall s\ \mathtt{sat}_\phi(s) \leftrightarrow \frac{1}{2} \cdot \left(\mathtt{sat}_{\phi'}(\mathtt{left}(s)) + \mathtt{sat}_{\phi'}(\mathtt{right}(s))\right) \bowtie \lambda$~~

    $\rightarrow$ Only the next real state is meaningful!

# Encoding a PCTL formula

$\mathtt{sat}_\phi : \mathtt{States} \to \mathbb{B}$, $\forall\phi$ subformula of $\psi$

- constraints on $\mathtt{sat}_\phi$ depend on the type of $\phi$

- Next operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\bigcirc\phi')$
  - ~~$\forall s\ \mathtt{sat}_\phi(s) \leftrightarrow \frac{1}{2}\cdot\left(\mathtt{sat}_{\phi'}(\mathtt{left}(s)) + \mathtt{sat}_{\phi'}(\mathtt{right}(s))\right) \bowtie \lambda$~~

    $\to$ Only the next real state is meaningful!
  - $\mathtt{value}_\phi : \mathtt{States} \to [0,1]$
    - $\forall s\ \mathtt{real}(s) \wedge \mathtt{sat}_{\phi'}(s) \to \mathtt{value}_\phi(s) = 1$
    - $\forall s\ \mathtt{real}(s) \wedge \neg\mathtt{sat}_{\phi'}(s) \to \mathtt{value}_\phi(s) = 0$
    - $\forall s\ \neg\mathtt{real}(s) \to \mathtt{value}_\phi(s) =$

      $$\frac{1}{2}\cdot\left(\mathtt{value}_\phi(\mathtt{left}(s)) + \mathtt{value}_\phi(\mathtt{right}(s))\right)$$

# Encoding a PCTL formula

$\mathtt{sat}_\phi : \mathtt{States} \to \mathbb{B}$, $\forall\phi$ subformula of $\psi$

- constraints on $\mathtt{sat}_\phi$ depend on the type of $\phi$

- Next operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\bigcirc\phi')$
  - ~~$\forall s\ \mathtt{sat}_\phi(s) \leftrightarrow \frac{1}{2} \cdot \left(\mathtt{sat}_{\phi'}(\mathtt{left}(s)) + \mathtt{sat}_{\phi'}(\mathtt{right}(s))\right) \bowtie \lambda$~~

    $\to$ Only the next real state is meaningful!
  - $\mathtt{value}_\phi : \mathtt{States} \to [0,1]$
    - $\forall s\ \mathtt{real}(s) \wedge \mathtt{sat}_{\phi'}(s) \to \mathtt{value}_\phi(s) = 1$
    - $\forall s\ \mathtt{real}(s) \wedge \neg\mathtt{sat}_{\phi'}(s) \to \mathtt{value}_\phi(s) = 0$
    - $\forall s\ \neg\mathtt{real}(s) \to \mathtt{value}_\phi(s) =$

      $$\frac{1}{2} \cdot \left(\mathtt{value}_\phi(\mathtt{left}(s)) + \mathtt{value}_\phi(\mathtt{right}(s))\right)$$
  - $\forall s\ \mathtt{sat}_\phi(s) \leftrightarrow \frac{1}{2} \cdot \left(\mathtt{value}_\phi(\mathtt{left}(s)) + \mathtt{value}_\phi(\mathtt{right}(s))\right) \bowtie \lambda$

# Encoding a PCTL formula (cont'd)

- Until operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\phi_1 \mathsf{U} \phi_2)$
  - $\mathtt{value}_\phi : \mathtt{States} \to [0,1]$

# Encoding a PCTL formula (cont'd)

- Until operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\phi_1 \mathsf{U} \phi_2)$
  - $\mathtt{value}_\phi : \mathtt{States} \to [0,1]$
    - $\forall s\ \mathtt{real}(s) \wedge \mathtt{sat}_{\phi_2}(s) \to \mathtt{value}_\phi(s) = 1$
    - $\forall s\ \mathtt{real}(s) \wedge \neg\mathtt{sat}_{\phi_1}(s) \wedge \neg\mathtt{sat}_{\phi_2}(s) \to \mathtt{value}_\phi(s) = 0$
    - $\forall s\ \neg\mathtt{real}(s) \vee \left(\mathtt{sat}_{\phi_1}(s) \wedge \neg\mathtt{sat}_{\phi_2}(s)\right) \to$
      $\mathtt{value}_\phi(s) = \frac{1}{2} \cdot (\mathtt{value}_\phi(\mathtt{left}(s)) + \mathtt{value}_\phi(\mathtt{right}(s)))$

# Encoding a PCTL formula (cont'd)

- Until operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\phi_1 \mathsf{U} \phi_2)$
  - $\mathtt{value}_\phi : \mathtt{States} \rightarrow [0,1]$
    - $\forall s\ \mathtt{real}(s) \wedge \mathtt{sat}_{\phi_2}(s) \rightarrow \mathtt{value}_\phi(s) = 1$
    - $\forall s\ \mathtt{real}(s) \wedge \neg\mathtt{sat}_{\phi_1}(s) \wedge \neg\mathtt{sat}_{\phi_2}(s) \rightarrow \mathtt{value}_\phi(s) = 0$
    - $\forall s\ \neg\mathtt{real}(s) \vee \left(\mathtt{sat}_{\phi_1}(s) \wedge \neg\mathtt{sat}_{\phi_2}(s)\right) \rightarrow$
      $\mathtt{value}_\phi(s) = \frac{1}{2} \cdot (\mathtt{value}_\phi(\mathtt{left}(s)) + \mathtt{value}_\phi(\mathtt{right}(s)))$
  - $\mathtt{dist}_\phi : \mathtt{States} \rightarrow [0,1]$ to ensure $\phi_2$ is reached w. positive proba
    - $\forall s\ \mathtt{real}(s) \wedge \mathtt{sat}_{\phi_2}(s) \leftrightarrow \mathtt{dist}_\phi(s) = 0$
    - $\forall s\ \mathtt{value}_\phi(s) = 0 \leftrightarrow \mathtt{dist}_\phi(s) = 1$
    - $\forall s\ \mathtt{value}_\phi(s) \neq 0 \wedge \left(\neg\mathtt{real}(s) \vee \neg\mathtt{sat}_{\phi_2}(s)\right) \rightarrow$
      $\left(\mathtt{dist}_\phi(s) > \mathtt{dist}_\phi(\mathtt{left}(s))\right) \vee \left(\mathtt{dist}_\phi(s) > \mathtt{dist}_\phi(\mathtt{right}(s))\right)$

# Encoding a PCTL formula (cont'd)

- Until operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\phi_1 \mathsf{U} \phi_2)$
  - $\mathtt{value}_\phi : \mathtt{States} \to [0,1]$
    - $\forall s\ \mathtt{real}(s) \land \mathtt{sat}_{\phi_2}(s) \to \mathtt{value}_\phi(s) = 1$
    - $\forall s\ \mathtt{real}(s) \land \neg\mathtt{sat}_{\phi_1}(s) \land \neg\mathtt{sat}_{\phi_2}(s) \to \mathtt{value}_\phi(s) = 0$
    - $\forall s\ \neg\mathtt{real}(s) \lor \left(\mathtt{sat}_{\phi_1}(s) \land \neg\mathtt{sat}_{\phi_2}(s)\right) \to$ $\mathtt{value}_\phi(s) = \frac{1}{2} \cdot (\mathtt{value}_\phi(\mathtt{left}(s)) + \mathtt{value}_\phi(\mathtt{right}(s)))$
  - $\mathtt{dist}_\phi : \mathtt{States} \to [0,1]$ to ensure $\phi_2$ is reached w. positive proba
    - $\forall s\ \mathtt{real}(s) \land \mathtt{sat}_{\phi_2}(s) \leftrightarrow \mathtt{dist}_\phi(s) = 0$
    - $\forall s\ \mathtt{value}_\phi(s) = 0 \leftrightarrow \mathtt{dist}_\phi(s) = 1$
    - $\forall s\ \mathtt{value}_\phi(s) \neq 0 \land \left(\neg\mathtt{real}(s) \lor \neg\mathtt{sat}_{\phi_2}(s)\right) \to$ $\left(\mathtt{dist}_\phi(s) > \mathtt{dist}_\phi(\mathtt{left}(s))\right) \lor \left(\mathtt{dist}_\phi(s) > \mathtt{dist}_\phi(\mathtt{right}(s))\right)$
  - $\forall s\ \mathtt{sat}_\phi(s) \leftrightarrow \mathtt{real}(s) \land \mathtt{value}_\phi(s) \bowtie \lambda.$

# Encoding a PCTL formula (cont'd)

- Until operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\phi_1 \mathsf{U} \phi_2)$
  - $\mathtt{value}_\phi : \mathtt{States} \to [0,1]$
    - $\forall s\ \mathtt{real}(s) \wedge \mathtt{sat}_{\phi_2}(s) \to \mathtt{value}_\phi(s) = 1$
    - $\forall s\ \mathtt{real}(s) \wedge \neg\mathtt{sat}_{\phi_1}(s) \wedge \neg\mathtt{sat}_{\phi_2}(s) \to \mathtt{value}_\phi(s) = 0$
    - $\forall s\ \neg\mathtt{real}(s) \vee \left(\mathtt{sat}_{\phi_1}(s) \wedge \neg\mathtt{sat}_{\phi_2}(s)\right) \to$
      $\mathtt{value}_\phi(s) = \frac{1}{2} \cdot (\mathtt{value}_\phi(\mathtt{left}(s)) + \mathtt{value}_\phi(\mathtt{right}(s)))$
  - $\mathtt{dist}_\phi : \mathtt{States} \to [0,1]$ to ensure $\phi_2$ is reached w. positive proba
    - $\forall s\ \mathtt{real}(s) \wedge \mathtt{sat}_{\phi_2}(s) \leftrightarrow \mathtt{dist}_\phi(s) = 0$
    - $\forall s\ \mathtt{value}_\phi(s) = 0 \leftrightarrow \mathtt{dist}_\phi(s) = 1$
    - $\forall s\ \mathtt{value}_\phi(s) \neq 0 \wedge \left(\neg\mathtt{real}(s) \vee \neg\mathtt{sat}_{\phi_2}(s)\right) \to$
      $\left(\mathtt{dist}_\phi(s) > \mathtt{dist}_\phi(\mathtt{left}(s))\right) \vee \left(\mathtt{dist}_\phi(s) > \mathtt{dist}_\phi(\mathtt{right}(s))\right)$
  - $\forall s\ \mathtt{sat}_\phi(s) \leftrightarrow \mathtt{real}(s) \wedge \mathtt{value}_\phi(s) \bowtie \lambda.$
- Bounded until operator: generalisation of next operator.

# Encoding a PCTL formula (cont'd)

- Until operator: $\phi = \mathbb{P}_{\bowtie\lambda}(\phi_1 \mathsf{U} \phi_2)$
  - $\mathtt{value}_\phi : \mathtt{States} \to [0,1]$
    - $\forall s\ \mathtt{real}(s) \wedge \mathtt{sat}_{\phi_2}(s) \to \mathtt{value}_\phi(s) = 1$
    - $\forall s\ \mathtt{real}(s) \wedge \neg\mathtt{sat}_{\phi_1}(s) \wedge \neg\mathtt{sat}_{\phi_2}(s) \to \mathtt{value}_\phi(s) = 0$
    - $\forall s\ \neg\mathtt{real}(s) \vee \big(\mathtt{sat}_{\phi_1}(s) \wedge \neg\mathtt{sat}_{\phi_2}(s)\big) \to$
      $\mathtt{value}_\phi(s) = \frac{1}{2} \cdot (\mathtt{value}_\phi(\mathtt{left}(s)) + \mathtt{value}_\phi(\mathtt{right}(s)))$
  - $\mathtt{dist}_\phi : \mathtt{States} \to [0,1]$ to ensure $\phi_2$ is reached w. positive proba
    - $\forall s\ \mathtt{real}(s) \wedge \mathtt{sat}_{\phi_2}(s) \leftrightarrow \mathtt{dist}_\phi(s) = 0$
    - $\forall s\ \mathtt{value}_\phi(s) = 0 \leftrightarrow \mathtt{dist}_\phi(s) = 1$
    - $\forall s\ \mathtt{value}_\phi(s) \neq 0 \wedge \big(\neg\mathtt{real}(s) \vee \neg\mathtt{sat}_{\phi_2}(s)\big) \to$
      $\big(\mathtt{dist}_\phi(s) > \mathtt{dist}_\phi(\mathtt{left}(s))\big) \vee \big(\mathtt{dist}_\phi(s) > \mathtt{dist}_\phi(\mathtt{right}(s))\big)$
  - $\forall s\ \mathtt{sat}_\phi(s) \leftrightarrow \mathtt{real}(s) \wedge \mathtt{value}_\phi(s) \bowtie \lambda.$
- Bounded until operator: generalisation of next operator.

- Global constraint: $\mathtt{real}(1) \wedge \mathtt{sat}_\psi(1)$.

# Experiments

A lossy channel specification

- *n* users sending messages over lossy channel.
- Formula for $n$ users has a model with $n+1$ states.
- 6 users: more than two hours.

Does not scale in model size!

$\rightarrow$ Not suitable for synthesis from specification.

# Experiments

## A lossy channel specification

- $n$ users sending messages over lossy channel.
- Formula for $n$ users has a model with $n + 1$ states.
- 6 users: more than two hours.

Does not scale in model size!

$\rightarrow$ Not suitable for synthesis from specification.

## A buggy lossy channel specification

- Formula for $n$ users has a model with 4 states.
- Hundreds of users / probabilistic operators: less than 1 hour.

Scales in formula size.

$\rightarrow$ Useful for “sanity” check.

# Conclusion

PCTL satisfiability

- long-standing open problem
- no finite model property, already for qualitative fragment

Contribution

- focus on simple and small models
- satisfiability check and model construction using SMT solver
- useful for sanity check rather than synthesis
- adaptable to qualitative PCTL satisfiability